FILED
J N DEC 04, 2007
DEC X 4 2007

MICHAEL W. DOBBINS
CLERK, U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA	)	07CR 792
	)	
vs.	)	No. ________________
	)	Violation: Title 18, United
KEITH WILSON	)	States Code, Section 1343

JUDGE GOTTSCHALL

MAGISTRATE JUDGE DENLOW

The UNITED STATES ATTORNEY charges:

1. At times material to this information:

a. DirecTV, Inc. (hereinafter "DirecTV") was a California corporation engaged in the business of delivering satellite television programming to its subscribers. DirecTV delivered television programming to the homes and businesses of its subscribers in the United States equipped with DirecTV satellite signal receiving equipment. That equipment included a satellite dish (hereinafter "Dish"), an integrated receiver/decoder (hereinafter "Receiver") and a DirecTV access card (hereinafter "Access Card") which is necessary to operate the Receiver.

b. Consumers who purchased DirecTV equipment could subscribe to various packages of DirecTV programming for which the subscriber paid a periodic fee, usually monthly. A subscriber also could order pay-per-view events and movies.

c. DirecTV contracted with and paid program providers such as cable networks, motion picture distributors, sports leagues, event promoters, and other programming rights holders, for the right to distribute their programming to its subscribers.

d. All programming distributed by DirecTV was delivered to DirecTV's broadcast centers in Castle Rock, Colorado, and Los Angeles, California. At the broadcast centers DirecTV digitized and compressed the programming. The resulting signal was encrypted, that is,

electronically scrambled by DirecTV to prevent unauthorized reception. DirecTV then transmitted the signal to five satellites located in stationary orbit approximately 22,300 miles above the equator.

e. The satellites relayed the encrypted signal back to earth where it could be received by DirecTV's subscribers. The satellite signal was received by each subscriber's Dish and transmitted by wire communication to the Receiver. The Receiver acted like a computer to process the incoming signal using information from the credit card sized Access Card.

f. Each Access Card contained a computer chip with copyrighted software and a unique electronic identifying number. The Access Card controlled which DirecTV programming the subscriber received unscrambled based on the programming package purchased by the subscriber. It also captured and transmitted to DirecTV the subscriber's pay-per-view orders.

g. The Receiver contained a computer microprocessor and proprietary verification software. This proprietary verification software made a comparison approximately every eight seconds between a unique code transmitted continuously with each DirecTV program and an authorization code generated using the Access Card to confirm that the subscriber was authorized to receive that program.

h. Various illicit devices were produced and sold to allow the unscrambling of DirecTV programming without authorization from or the payment of subscription fees to DirecTV. These devices were used to modify the Access Cards and provide materially false information to the proprietary verification software contained in Receivers by misrepresenting the authorized programming status of the Access Card.

i. To combat the use of these illicit devices, DirecTV began to periodically disseminate so-called "electronic counter measures" (hereinafter sometimes "ECMs"). ECMs were

electronic messages sent through the satellite data stream to deactivate the illicit Access Cards. Some of the ECMs corrupted or "looped" the "pirate" software in the illicit Access Cards to make them inoperable. The "pirate community" developed "unlooper" devices, which could restore the software in the "looped" Access Cards to allow them to again be illicitly programmed to decrypt all DirecTV's satellite signals.

j. To further combat the use of these illicit Access Cards, DirecTV initiated a replacement of its original Access Cards. New, more secure, Access Cards, sometimes known as "H cards" or "HU Cards" were sent to all DirecTV subscribers.

k. DirecTV held copyrights to its satellite television programming delivery system("the copyrighted work").

2. From in or about August 2001 to at least in or about March 2002, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,

KEITH WILSON

defendant herein, and others both known and unknown to the Grand Jury, devised and intended to devise a scheme and artifice to defraud and for obtaining property by means of false and fraudulent representations from DirecTV.

The Scheme to Defraud

3. It was part of the scheme that the defendant did sell and distribute devices, the primary and intended purposes of which were to assist in the decryption of all DirecTV satellite television programming without payment of the required subscription fees and pay-per-view fees. These devices (hereinafter sometimes referred to as the "Devices") included "unloopers", "bootloaders", "emulators" and other related devices.

a. The "unloopers" were devices designed to modify DirecTV "H Cards" that previously had been deactivated by an electronic counter measure in order that those Access Cards could be reprogrammed to enable viewing of all DirecTV channels without payment of the required subscription fees or pay-per-view fees to DirecTV.

b. The "bootloaders" were devices designed to modify DirecTV "HU Cards" to enable viewing of all DirecTV channels without payment of the required subscription fees or pay-per-view fees to DirecTV.

c. The "emulators" were printed circuit boards designed for use with an Intel based computer and special software to emulate a DirecTV "H Card", which allowed a user to view all DirecTV channels without payment of the required subscription fees or pay-per-view fees to DirecTV.

4. It was further part of this scheme that the defendant intended that the purchasers of the Devices, specifically the HU Loaders and unloopers, would be used by the purchasers to modify the Access Cards and provide materially false information to the proprietary verification software contained in Receivers by misrepresenting the authorized programming status of the Access Card. This enabled the purchasers to decrypt DirecTV's satellite television programming without payment of the required subscription fees or pay-per-view fees.

5. It was further part of the scheme that the defendant paid Individual A to manufacture some of the Devices he sold and distributed.

6. It was further part of the scheme that the defendant advertised the Devices on Internet websites, including www.dssdragon.com, www.dssoutpost.com , and www.industry.com.

7. It was further part of the scheme that the defendant, and others acting at his direction,

received orders for the Devices via the telephone and via electronic mail messages from individuals in Illinois, other states and Canada and shipped the Devices to those individuals via United Parcels Service.

8. It was further part of the scheme that the defendant collected the payments for the sold Devices through Internet based payment services and through Cash on Delivery shipments of the Devices. Internet and COD payments were credited to a Digital Smartcard Security, an Illinois corporation owned and operated by the defendant.

9. It was further part of the scheme that the defendant received 2,935 orders for 4,695 Devices to advertised on www.dssdragon.com, www.dssoutpost.com, and www.industry.com.

10. It was further part of the scheme that the defendant opened a bank account, under the name of Digital Smartcard Security, at Bank One, in Chicago, Illinois, for purposes of receiving credits for COD payments.

11. On or about March 22, 2002, at Chicago, in the Northern District of Illinois, Eastern Division,

KEITH WILSON,

defendant herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce from Atlanta, Georgia to Chicago, Illinois, certain signs, signals and sounds, namely: an electronic transfer of funds to defendant's bank account in the name of Digital Smartcard Security, at Bank One, in the amount of $134.59;

In violation of Title 18, United States Code, Sections 1343 and 2.

Count Two

The UNITED STATES ATTORNEY further charges:

1. The UNITED STATES ATTORNEY realleges and incorporates by reference paragraphs 1 through 10 of Count One of the Information.

2. On or about March 25, at Chicago, in the Northern District of Illinois, Eastern Division,

KEITH WILSON,

defendant herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce from Atlanta, Georgia to Chicago, Illinois, certain signs, signals and sounds, namely: an electronic transfer of funds to defendant's bank account in the name of Digital Smartcard Security, at Bank One, in the amount of $184.44;

In violation of Title 18, United States Code, Sections 1343 and 2.

Count Three

The UNITED STATES ATTORNEY further charges:

1. The UNITED STATES ATTORNEY realleges and incorporates by reference paragraphs 1 through 10 of Count One of the Information.

2. On or about March 26, at Chicago, in the Northern District of Illinois, Eastern Division,

KEITH WILSON,

defendant herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce from Atlanta, Georgia to Chicago, Illinois, certain signs, signals and sounds, namely: an electronic transfer of funds to defendant's bank account in the name of Digital Smartcard Security, at Bank One, in the amount of $393.81;

In violation of Title 18, United States Code, Sections 1343 and 2.

Patrick J. Fitzgerald
United States Attorney